Journal of Information Security, 2017, 8, 141-165
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

An Innovative Soft Design Science Methodology for Improving Development of a Secure Information System in Tanzania Using Multi-Layered Approach

Maduhu Mshangi[1*], Edephonce Ngemera Nfuka[2], Camilius Sanga[3]

[1]NECTA, Dar es Salaam, Tanzania
[2]Open University of Tanzania, Dar es Salaam, Tanzania
[3]Sokoine University of Agriculture, Morogoro, Tanzania
Email: *mshangimaduhu@yahoo.com

How to cite this paper: Mshangi, M., Nfuka, E.N. and Sanga, C. (2017) An Innovative Soft Design Science Methodology for Improving Development of a Secure Information System in Tanzania Using Multi-Layered Approach. *Journal of Information Security*, **8**, 141-165.
https://doi.org/10.4236/jis.2017.83010

Received: May 5, 2017
Accepted: July 3, 2017
Published: July 6, 2017

Abstract

This paper presents an innovative Soft Design Science Methodology for improving information systems security using multi-layered security approach. The study applied Soft Design Science Methodology to address the problematic situation on how information systems security can be improved. In addition, Soft Design Science Methodology was compounded with mixed research methodology. This holistic approach helped for research methodology triangulation. The study assessed security requirements and developed a framework for improving information systems security. The study carried out maturity level assessment to determine security status quo in the education sector in Tanzania. The study identified security requirements gap (IT security controls, IT security measures) using ISO/IEC 21827: Systems Security Engineering-Capability Maturity Model (SSE-CMM) with a rating scale of 0 - 5. The results of this study show that maturity level across security domain is 0.44 out of 5. The finding shows that the implementation of IT security controls and security measures for ensuring security goals are lacking or conducted in ad-hoc. Thus, for improving the security of information systems, organisations should implement security controls and security measures in each security domain (multi-layer security). This research provides a framework for enhancing information systems security during capturing, processing, storage and transmission of information. This research has several practical contributions. Firstly, it contributes to the body of knowledge of information systems security by providing a set of security requirements for ensuring information systems security. Secondly, it contributes empirical evidence on how information systems security can be improved. Thirdly, it contributes on the applica-

bility of Soft Design Science Methodology on addressing the problematic situation in information systems security. The research findings can be used by decision makers and lawmakers to improve existing cyber security laws, and enact laws for data privacy and sharing of open data.

Keywords

Soft Design Science, Information Systems Security, Design Science Research, Soft Systems Methodology, Multi-Layered Approach

1. Introduction

The advancement of information communication technologies (ICT) enabled the integration of information systems in cyberspace which is accessible through the Internet and mobile based platforms. Recently, researchers have shown an increased number of cyber crimes affecting information systems in cyberspace. A study by [1] revealed that 12.8% of users in the education sector in Tanzania experience cyber-attacks due to visiting unhealthy websites; 63.29% of e-mails received by users are spam. Thus, security of information in information systems during capturing, processing, storage, and transmission is questionable. This is evidenced by past studies, such as [2] argued that the number of security incidents exploiting security holes in the information systems in cyberspace is increasing. One of the notable security holes is a heart-bleed attack. A study by [2] found that 89% of the universities information systems in cyberspace were vulnerable to heart-bleed attack. The heart-bleed attack is the vulnerability in Open SSL cryptographic software, and allows stealing of the protected information such as username, password, and private certificates in memory of the computer.

Further, [3] argued that many systems security problems are contributed by lack of integrating systematic research methodology, standard security guideline, and principles, security awareness training, and secure coding practices in systems development life cycle. A study by [3] revealed that security awareness training is lacking or conducted in ad-hoc with a mean of 0.59 and standard deviation of 0.499 in rating scale of 0 - 5 of the System Security Engineering Capability Maturity Model (SSE-CMM).A study by [3] revealed that secure coding is non-existence or practiced in ad-hoc; with a mean of 0.33 and standard deviation of 0.516 in rating scale of 0 - 5 of SSE-CMM. These contribute to the problem of the insecure systems which requires security improvement to ensure security goals (confidentiality, integrity, and availability) are guaranteed. These security problems are contributed by human factor involvement in security. According to a study by [3], come out with the integration of Soft System Methodology and Design Science Research in solving information systems security problematic situation. The results of this integration termed as Soft Design Science Methodology; it has been employed in this study to tackle a problematic situation on how information systems security (ISS) can be improved.

Different approaches have been employed in tackling this wicked problematic

situation on how ISS can be improved. These approaches lack multi-layered security integration with Soft Design Science Methodology. Many people make the mistake of believing that building security into information systems (ISs) is simply a matter of referring to a checklist [4] of technical and procedural controls and applying the appropriate security measures on the list. The checklist approach also fails [4]; because many people focus on checking that the links in the chain exist but do not test that the links actually fit together to form a secure chain system. Thus, various studies have tried to address this problem on how to improve the security of information in information systems; but these approaches lack multi-layered security integration with Soft Design Science Methodology. Thus, the current study addresses the messy problematic situation on how ISS can be improved; using multi-layers security integration with Soft Design Science Methodology. This is a methodology for tackling real world messy problematic situation involving human factor, such as how to improve information systems security.

This research has several practical contributions. Firstly, it contributes to the body of knowledge of information systems security by providing a set of security requirements for ensuring information systems security. Secondly, it contributes empirical evidence on how information systems security can be improved. Thirdly, it contributes on the applicability of Soft Design Science Methodology on addressing the problematic situation in information systems security. Fourthly, this research provides a framework for enhancing information systems security during capturing, processing, storage and transmission of information.

The paper is organized as follows: Section 1: presents an introduction, problem statement, and main research objective and research question. Section 2 presents the related works, the theoretical foundations of research methodology: Soft Design Science Methodology, and research gap. Section 3 presents the materials and methods employed in this study. Section 4 presents the root definition of the problem and requirement analysis using CATWOE analysis. Section 5 presents the results findings and discussion. Section 6 describes the proposed framework for tackling real world problematic situation and filling in the identified research gap. Section 7 presents the research study contributions in this study. Finally, section 8 presents the conclusion and recommendations.

1.1. Problem Statement

Information systems security (ISS) is the protection of information and information systems (ISs) from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability [5] [6]. Information security management incorporates the identification of information resources used by organisations, development, and implementation of policies, standards, guidelines, and procedures to protect those resources (assets) [5]. Ensuring ISS, by ensuring security goals (confidentiality, integrity, and availability) of information manipulated by computing systems is a long-standing yet increasingly wicked, messy ill-defined problematic situation

facing information systems in cyberspace. The numerous technical advances in ICT do not always produce more secure environments for information systems in cyberspace. Therefore, the information systems security problem in cyberspace cannot be understood or described as solely a technical problem. Information systems are operated by people and this means that information systems security is also a human factor issue [7] [8] [9] [10]. Human factors influence how individuals interact with information systems security technology; it is this interaction that is often detrimental to the security of information systems in cyberspace [10]. The threats/risks resulted from human factors includes cybercrimes such as hacking, phishing attacks, SMiShing attacks, social engineering attacks, insider attacks (employees sabotages, consultants, contractors, vendors), data theft and leakages [5] [10] [11].

The existing models, frameworks, and standards for addressing the security of information systems in cyberspace are inadequate [4] [5] [12]-[22] practical techniques for enforcing them are unsatisfactory. Within an information system, for any given moment, information is found in one or more of the four states; during capturing, processing, storage, and transmission. The security requirements for ensuring the security of information in information systems should be defined in each information states. Ensuring security of information during capturing, processing, storage, and transmission in information systems is debatable due to failure to ensure security goals (confidentiality, integrity, and availability) in information systems. The solution for tackling a problematic situation involving human factor, need a multi-layer security approach integration with Soft Design Science Methodology. The main research problem is to tackle the real world messy, wicked problematic situation involving human factor; how information systems security can be improved, the case of the education sector in Tanzania. The study adopted Soft Design Science Methodology to guide the research process.

1.2. Objective of Study

The main objective of this study was to tackle the messy, wicked, complex problematic situation on how information systems security can be improved. The study assessed security requirements and developed a framework for improving the security of information during capturing, processing, storage and transmission in information systems; using multi-layered security approach integration with Soft Design Science Methodology.

2. Related Works and Theoretical Foundations of Research Methodology

This section presents the related works to this study and the methodology employed to guide the research work.

2.1. Related Works

Various studies have tried to address the problem of how information systems

security can be improved, using different approaches. Some of these studies include, a study by [12] focused on improvement of the ICT security management process in non-commercial organisations. A study by [15] proposed framework using rule-based approach. A study by [23] proposed a multi-layer model for e-government information security assessment. A study by [24] focused on enhancing the governance of information security in developing countries (the case of Zanzibar). All these studies lacked the soft system thinking multi-layer security integration approach. This approach is effective for tackling wicked, messy problematic situation involving human factor. Any security system, no matter how well designed and implemented, will have to rely on people [10]. The human factors play a crucial part in the majority of security incidents affecting information systems in cyberspace. Implementing appropriate technical solutions alone still, fail to handle the human factor which results in insecure systems [10] [11].

The existing models, frameworks, and standards have limitations. For example, SABSA [4], ISO27001/2 [13] [14], McCumber [16] and COBIT 5 [25] [26] for information security have limitations. These standards, frameworks or models are too general, need customization and are based on the general environment not targeted environment (education sector in Tanzania). Thus, some have limitations with respect to the research problem and research objective. Today's sophisticated attacker's strike across multiple layers. That means that our security must also be layered. Layered security refers to security systems that use multiple components to protect operations on multiple levels or layers [27]. Multi-layered security approach without integration with the soft system thinking approach is ineffective for addressing the wicked, complex problematic situation involving human factor. Thus, to address the wicked, complex problematic situation involving human factor, such as how information systems security can be improved; the study adopted multi-layered security approach integration with Soft Design Science Methodology.

2.2. Theoretical Foundations of Research Methodology: Soft Design Science Methodology

The Soft Design Science Methodology [3] [28] merges the common Design Science Research (DSR) process (design, build-artifact, evaluation) [29] [30] together with the iterative Soft Systems Methodology (SSM). The design-build artifact evaluation process was iterated until the specific requirements were met [31] (**Figure 1** and **Figure 2**).

2.2.1. Design Science Research

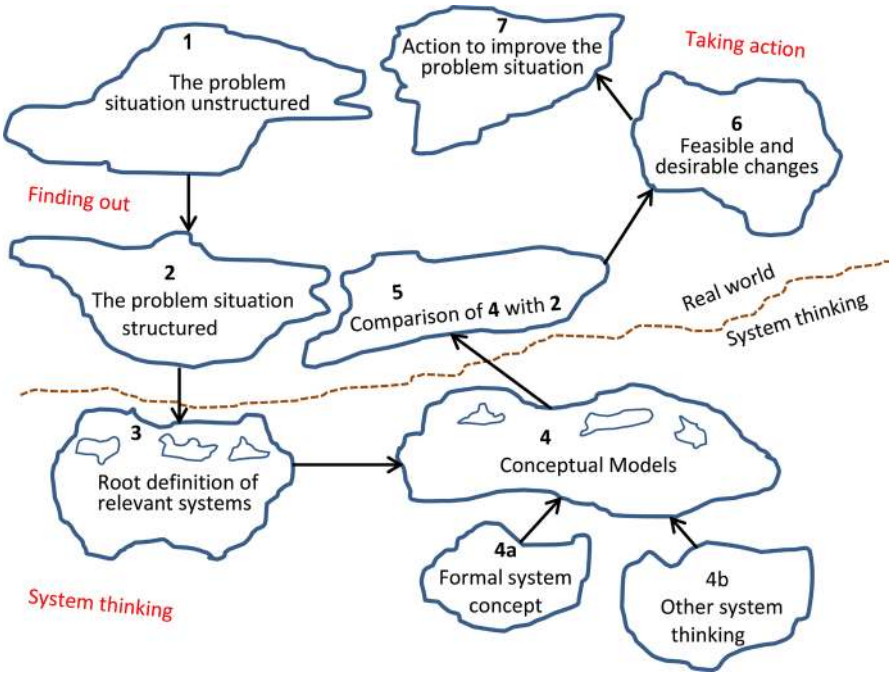
Design Science Research (DSR) is the research methodology used for creation and evaluation of artifacts for information models (abstractions, architects, frameworks, conceptual systems intended to solve an identified fuzzy organisational problem [32] [33] [34] using behavioural and design science paradigms [33] [35]. Information systems artifacts are broadly defined as constructs (vocabulary and symbols) [36], models, representations, methods (algorithms and

practices), and instantiations (implementation of systems, and prototype systems) [36]. The design is a wicked problem by itself based on the following criteria: requirements and constraints are unstable; complex interactions among subcomponents of the problem and resulting subcomponents of the solution; inherent flexibility to change artifacts and processes; dependence on human cognitive abilities and dependence on human social abilities. DSR has gained significant acceptance within the design work on technology solution but it lacks the socio-technical concern [35] [37] which is a vital component in the conceptualization of artifact development. In this study, the weakness of DSR was addressed by the strength of Soft Systems Methodology and vice versa (**Figure 1** and **Figure 2**).

2.2.2. Soft Systems Methodology

Soft Systems Methodology(SSM) is the methodology which assists people in solving a complex, messy problem in the organisation by using systems rules and principles that allow structuring your system thinking about the real world [38] [39]. The real world problematic situation in this study is how to improve the security of information during capturing, processing, storage, and transmission in information systems. At the heart of SSM is a comparison between the world as it is, and some models of the world as it might be [40]. Out of this comparison arise a better understanding of the world ("research") and some ideas for improvement ("action") [39] [40]. The SSM has seven stages; some of them address the real world, and some of them perhaps the most important parts address a conceptual world (**Figure 1**).

Applying the seven stages of SSM (**Figure 1**); soft systems thinking seeks to



Source: [39] [41].

Figure 1. Stages of SSM.

explore the "messy" problematic situations that arise in human activity [42] [43]. SSM is a process of seven stages of analysis which uses the concept of a system of human activity as a means to get from the "finding" of the problematic situation (wicked/complex problem) to "taking action" to improve the situation [31] [42]. The SSM has strengths and weaknesses. One of the strengths of SSM is in solving complex messy problematic situations. One of the weaknesses of SSM is that it does not deal with implementation issue [44] [45]. The SSM was integrated with DSR methodology (this integration formed Soft Design Science Methodology) [3]; the weaknesses of one were complemented by the strengths of other. In this study, Soft Design Science Methodology was employed in the design and development of a framework for enhancing information systems security. Soft Design Science Methodology was employed in the creation of this artifact. The developed artifact was compared with the real world in circular fashion (**Figure 1** and **Figure 2**) until an optimal framework for enhancing ISS was obtained.

2.3. Research Gap

The application of information security technologies does not always result in improved security for information systems in cyberspace. Technology is quite an essential part relating to securing information resources (assets) but people are responsible for design, implementation, and operation of these technological tools for enhancing information systems security during capturing, processing, storage, and transmission. The solution for tackling a problematic situation involving human factor, need a multi-layer security approach integration with Soft Design Science Methodology. There have been a number of valuable studies related to improving the security of information systems, such as studies by [12] [15] [16] [24] [35] [37] [46]-[51] and others. However, none of these studies were carried out for improving information systems security using multi-layered security approach integration with Soft Design Science Methodology.

These past studies have not addressed the identified research gap; for example, a study by [50] focused on ensuring security and privacy of electronic patient records (case of the hospital). A study by [15] proposed a framework based on Microsoft advanced analytics model [17] [18] (STRIDE threat model). This lacks soft systems thinking approach, and it is a vendor based model which implies extension to other environments, not guarantees to give desired results. A study by [24] proposed a framework for information security culture case of Zanzibar; this may not work in the education sector in Tanzania as culture differs from one sector to another. Hence, creates a research gap, for this study, on how the security of information systems in the education sector in Tanzania can be improved.

3. Materials and Methods

The study employed qualitative and quantitative research method for data collection [52] [53]. The quantitate methods employed were surveyed questionnaires (management staff, end users, and IT staff). The qualitative research me-

thods employed were semi-structure interview using electronic assessment tools [54] for focused group/individuals, participant observation and documentary review [55] [56]. The data collection was conducted in seven organisations under study in the education sector in Tanzania [57] [58]. The seven organisations selected are those which are mainly involved in the education assessment and management of education in Tanzania, because of their high impact on the whole sector. In this study, the names of the seven selected organisations referred as K, L, M, N, O, P and Q [57] [58] were not disclosed for confidentiality purpose. In this case, the level of analysis is organisational.

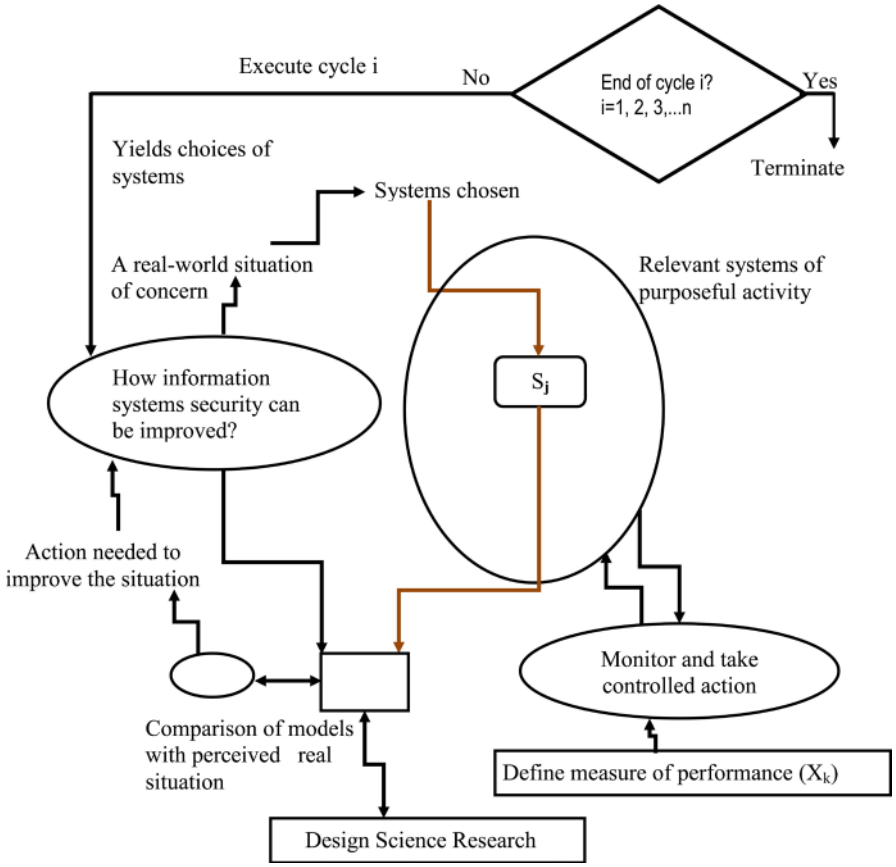
The research involved collection of quantitative and qualitative data from seven organisations (**Table 1**) to answer the research question, how can information systems security (ISS) be improved?. The sample size for this study was 154 respondents from seven organisations in the education sector. The distributions of these respondents are presented in **Table 1**. This sample was selected using purposive and stratified random sampling techniques. Purposive sampling relies on the judgment of the researcher when it comes to selecting the units (e.g., people, cases/organisations, events, pieces of data) that are to be studied [55] [56]. The selected respondents in this study were those involved in the managing of ICT and security of information systems; procurement decisions of ICT equipment/accessories; ICT use and compliances. The respondents were selected based on the organisation structure. Taking into account these aspects, the purposive sampling technique was the optimal choice for sampling design. The respondents (**Table 1**) were comprised of top management (Permanent Secretary, Commissioners, and Chief Executive Officers), senior management (Directors, Chief Financial Officers, Divisions/ Head of Departments), Operations management (Head of Units/Sections), ICT experts (Network/Systems Administrators, IT Security Specialists and other ICT Staff); and end users (operations staff who interact with information systems and know the business processes) from the 7 organisations under study.

A stratified random sampling was used to select respondents for end users of information systems from sampling frame (list of all end users of information systems for 7 organisations under study) based on the research question. The

Table 1. Respondents.

Respondents	Organisation							Total
	O	P	L	M	Q	K	N	
ICT staff	4	2	3	20	4	3	4	**40**
Management staff	4	5	4	21	6	5	5	**50**
End Users of information systems	2	3	4	19	5	2	3	**38**
Total Respondents (Sample)	**11**	**12**	**12**	**74**	**18**	**13**	**14**	**154**
Total Actual Respondents	**10**	**10**	**11**	**60**	**15**	**10**	**12**	**128**
Survey Response Rate%	**91%**	**83%**	**92%**	**81%**	**83%**	**77%**	**86%**	**83%**

Source: [57] [58].



Key: S_j *is the given system under improvement which undergo cycles of iterations* (i = 1, 2, 3, …); j = 1, 2, 3, …

Figure 2. How Soft Design Science Methodology was used in this study (adapted from [31] [42]).

sampling frame was divided into 7 strata (strata K, L, M, N, O, P, and Q) comprising of end users of information systems from 7 organisations. The respondents from each stratum were selected using random sampling [55] [56].

Due to the nature of the research problem, SSM (**Figure 2**) was adopted to manage the analysis of data in a systematic way and circular fashion. Collected data were first cleaned and coded before being analysed. In cycles i = 1, 2, 3 in **Figure 2**, the survey data were analysed to determine security requirements (IT security controls; security measures to ensure security goals of information security are guaranteed). The analysis was done in cycle i = 1 for management staff (Sj, j = 1); cycle i = 2 for ICT Staff (Sj, j = 2); cycle i = 3 for end user of information systems (Sj, j = 3). Out of these comparisons give relevance systems of purpose which require improvement. The validity and reliability of data were determined. The analysis of the collected data in each cycle (**Figure 2**) was done using "R statistical computing package" based on SSE-CMM [59]. R is a software language for carrying out complicated (and simple) statistical analyses [60] [61].

The SSE-CMM, with a rating scale of 0 - 5: minimum 0 and maximum 5 was used; 0—not performed (non-existent); 1—performed informally (unplanned/ad-hoc); 2—partially implemented (planned); 3—implementation is in progress

(planned and tracked); 4—fully implemented (well defined and auditable); 5—fully implemented and regularly updated (monitored and audited for compliance). Validity and reliability of data were controlled. Cronbach alpha [62] [63] was used to test the reliability of survey questionnaires. The Cronbach alpha in this study was found to be 0.901, which is above 0.7. Thus, survey questionnaires in this study were reliable. The analysis was repeated for semi-structured interview data, participant observation, and documentation review. The data were coded and analysed using R, managed by SSM (**Figure 2**) in a circular fashion for cycles i = 1, 2, 3… and Sj, j = 1, 2, 3 ... The findings from this study were described and presented in form of charts, figures, and graphs.

4. Root Definition of the Problem and Requirements Analysis

The problem root definition and requirements analysis were determined using CATWOE analysis. The CATWOE analysis was employed to determine root definition [42] of the complex, real world problematic situation on how to improve information systems security. The CATWOE [64] [65] is a mnemonic with 6 elements denoting **C**ustomer/Client, **A**ctors, **T**ransformation, **W**eltanschauung, **O**wner and **E**nvironmental Constraints.

The study applied the CATWOE analysis to tackle the problematic situation on how to improve ISS by asking at least three questions. The questions asked includes: *what the study is trying to achieve* (W)?; *How* (T)?; what constraints it (E)? [66] [67]. In answering what is the study is trying to achieve, CATWOE analysis was used to explore the security requirements for ensuring security goals (CIA) are guaranteed for information during capturing, processing, storage, and transmission in information systems. In answering the *how* (T) question of CATWOE analysis, the inputs were security requirements (IT security measures and security controls) [67]. The results of CATWOE analysis in this study are summarized in **Figure 3**.

5. Results and Discussions

The results findings for analysed data address the research question on "how the information systems security can be improved?" To address this research question, the study carried out an assessment of the institution information security maturity level to determine security requirements for improvement based on domain security maturity level. The security domains for improving ISS include risk management (ISO4); security policy (ISO5); organisation of information security (ISO6); asset management(ISO7); human resources security (ISO8); physical and environmental security(ISO9); communications and operations management (ISO10); access control(ISO11); information systems acquisition, development, and maintenance (ISO12); information security incident management (ISO13); business continuity management(ISO14); and compliance (ISO15).

The data analysis was managed by SSM (**Figure 2**) in a circular fashion by executing every cycle i for a given iteration cycle (i = 1, 2, 3, … n) for each secu-

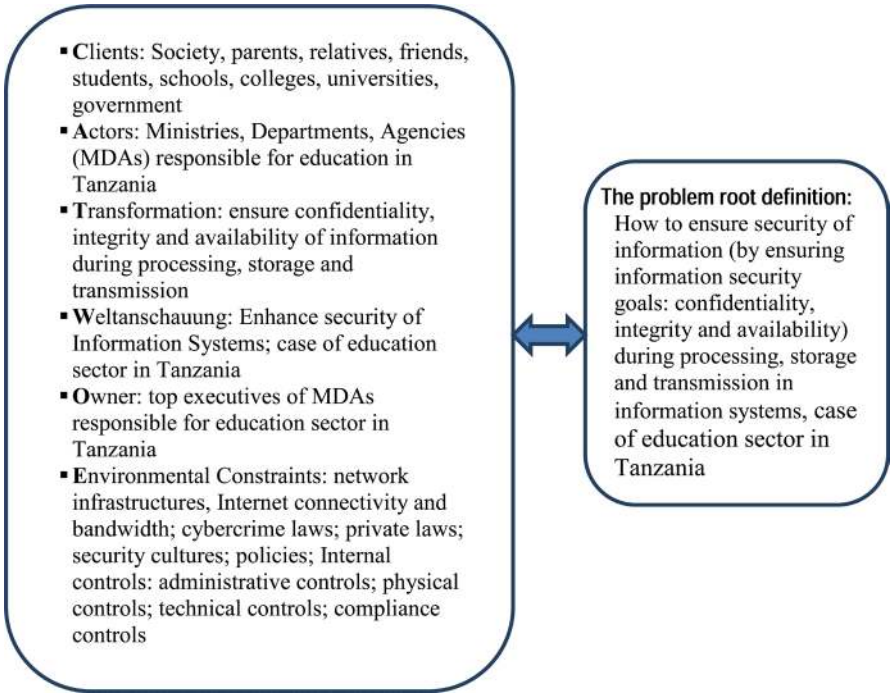


Figure 3. CATWOE analyses on how ISS can be improved (adapted from [67] [68]).

Table 2. Security domains maturity level.

Security domain	Organisation							Average	Implementation
	L	K	O	M	P	N	Q		
ISO4	0.5	0	3	2.5	0	0.5	0	0.93	19%
ISO5	0	0	0.67	0.67	0	0.67	0	0.29	6%
ISO6	0	0	0.67	0.67	0	0.33	0.33	0.29	6%
ISO7	1	0	1	0.5	0	1	1	0.64	13%
ISO8	0.4	0.4	0.8	0.4	0.4	0.8	0.8	0.57	11%
ISO9	1	0.5	0.75	0.75	0.5	0.75	0.75	0.71	14%
ISO10	0.74	0.37	0.42	1.05	0.11	0.37	0.84	0.56	11%
ISO11	0.67	0.08	0.42	0.58	0	0.17	0.5	0.35	7%
ISO12	0.38	0	0.5	0.75	0	0.25	0.5	0.34	7%
ISO13	0	0	0	0.5	0.5	0	0.5	0.21	4%
ISO14	1	0	0	0	1	0	0	0.29	6%
ISO15	0.25	0.25	0.25	0.25	0	0	0.25	0.18	4%
Overall maturity	0.49	0.13	0.71	0.72	0.2	0.39	0.44	0.44	9%

Source: [57] [58].

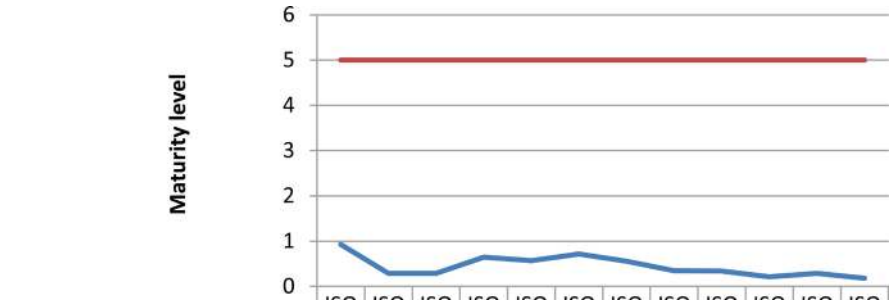
rity domain (j = 1, 2, 3, … n which correspond to ISO4, ISO5, ..., ISO13, ISO, 14, ISO15). The results finding depicts that maturity level across security domain is 0.44 (19%) out of 5 in SSE-CMM rating scale of 0 - 5 (Table 2). The finding shows that implementation of security controls/countermeasures for most in-

formation security domain is lacking. Thus, in order to improve the security of information systems, organisations should implement security controls/ countermeasures in each security domain.

The collected data were analysed and visualised using time line series graph to portray maturity level of seven organisations under study. From the graph (Figure 4), the study portrays that maturity level across domain is below 1 out of 5 in SSE-CMM rating scale 0 - 5. The highest maturity level is 0.93 for risk management (ISO4) and the lowest security domain maturity level is 0.18 for compliance (ISO15). The study found that maturity level across security domains is a time series graph with curve line having an average maturity between 0 and 1 out of 5 optimal maturity levels in SSE-CMM rating scale 0 - 5. Thus, ensuring the security of information systems in Tanzania education sector is questionable. For improving the security of information systems, organisations should implement security controls/countermeasures in each security requirement domain.

Further analysis was done using radar/spider chart analytical tool. The choice of radar analytical tool was based on the nature of research question which involved multivariate observations sharing similar characteristics (security maturity levels in SSE-CMM rating scale of 0 - 5). The radar chart was used to tackle the research question on how the information systems security can be improved. The radar chart was used to visualize multivariate observations for institutional maturity level across security requirements domains. Figure 5 depicts a radar chart for institutional security maturity across security requirement domains. The radar shows that the institutional security maturity is similar across security requirement domains centred within radii of less than 1 in SSE-CMM rating scale of 0 - 5 radii. Further, the study found that the highest radii are 3.0 for risk management (ISO4) in organisation O followed by the radius of 2.5 in organisation M. The rest of organisations under study have radii below 1.0 out of 5 in SSE-CMM rating scale of 0 - 5. For improving ISS, organisations should view security as a system with multi-layers composed of different security requirements domains interrelated to each other (Figure 5).

The study revealed that maturity level across security domain is 0.44 out of 5



	ISO 4	ISO 5	ISO 6	ISO 7	ISO 8	ISO 9	ISO 10	ISO 11	ISO 12	ISO 13	ISO 14	ISO 15
Security domain maturity	0.93	0.29	0.29	0.64	0.57	0.71	0.56	0.35	0.34	0.21	0.29	0.18
Optimal level	5	5	5	5	5	5	5	5	5	5	5	5

Figure 4. Line graph for institution security domain maturity [57] [58].

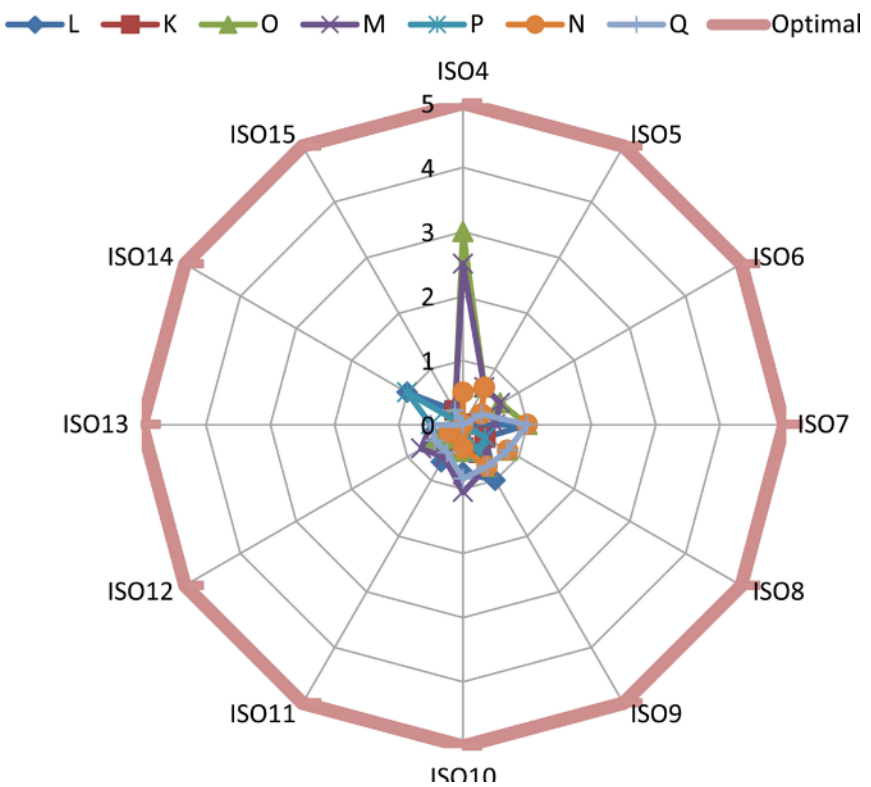


Figure 5. Radar for institution security domain maturity level [57] [58].

in SSE-CMM rating scale 0 - 5. The study found that information security maturity average across organisations is 0.44 out of 5 in SSE-CMM rating scale of 0 - 5.

The research findings further revealed that some of organisations websites/online information systems in the education sector in Tanzania have been hacked in the period of 2011-2016 due to the lack or ineffective IT security controls and security measures. For example, organisation "O" website and online application system were hacked on 2015-04-27:00:23. The organisation "P" website was hacked on 2015-07-31: 16:50. The organisation "L" website and central admission system were hacked on July 2014. The organisation "M" website was hacked on 2015-01-21:12:13. The organisation "K" website was hacked on 29/04/2011, and 14/08/2012. The organisation "K", foreign award assessment system was hacked on 2015/09/29:14:35. The hacking is due to organisations lack of implementing security controls such as security incidents not reported and handled effectively. This was contributed by organizations using open source software without shutting down open holes (vulnerabilities) and lack of IT security training. For example, online registration system was hacked by exploiting the CVE-2013-2586 XAMPP software (lang.php Write Into Local Disk method) vulnerability.

These findings are similar to earlier studies by [1] which found that information systems in cyberspace are affected by cybercrimes. Similarly, studies by [2] [3] found that the number of security incidents exploiting security holes in the web applications is increasing (e.g. the Heartbleed bug). Thus, the results of the

current study indicate that there is a lack or ad-hoc implementation of IT security controls and counter measures (for ensuring CIA) in information systems during capturing, processing, storage and transmission of information. Thus, IT security controls and security measures implementation is lacking or practiced in ad-hoc in most of the security domains. This security domain includes risk management; a security policy; organisation of information security; asset management security; human resources security; physical and environmental security; communications and operations management security; access control security; information systems acquisition, development, and maintenance; information security incident management; business continuity management; compliance. Thus, the study proposed a framework for enhancing information systems security (ISS).

6. Proposed Framework for Enhancing Information Systems Security

The Soft Design Science Methodology was employed to produce the desired artefact. The study employed the root problem definition (CATWOE analysis) (**Figure 3**).The results from research findings were applied in designing and creating of the innovative artefact for a proposed framework for enhancing information systems security. The process was iterated by comparing real world and the conceptual world until the specific requirements were met in the transformation process of developing a framework for enhancing information systems security during capturing, processing, storage, and transmission. **Figure 6** depicts the proposed framework for enhancing information systems security. This framework has been developed to address the main research problem: "how to ensure the security of information during capturing, processing, storage and transmission in information systems (ISs), the case of the education sector in Tanzania". The proposed framework for enhancing ISS (**Figure 6**) has been developed based on literature view, conceptual framework, research methodology, data collections, data analysis, research findings and security requirements.

The proposed framework for enhancing ISS, mainly comprise of the following components: information security services(security goals); information states; security measures for ensuring confidentiality, integrity, and availability of information; IT security controls; Soft Design Science Methodology(Design Science Research integrated with Soft System Methodology) (**Figure 6**).

i) Information security services(security goals)

The security services can be categorized as availability, integrity, authenticity, confidentiality, privacy, and non-repudiation. The framework presents three categories of information security services (security goals), namely: confidentiality, integrity, and availability. The others are included in these three categories. For, example, Integrity also covers Authenticity and non-repudiation. Confidentiality includes privacy dimension.

a) Confidentiality

Confidentiality is the prevention of the intentional or unintentional unau-

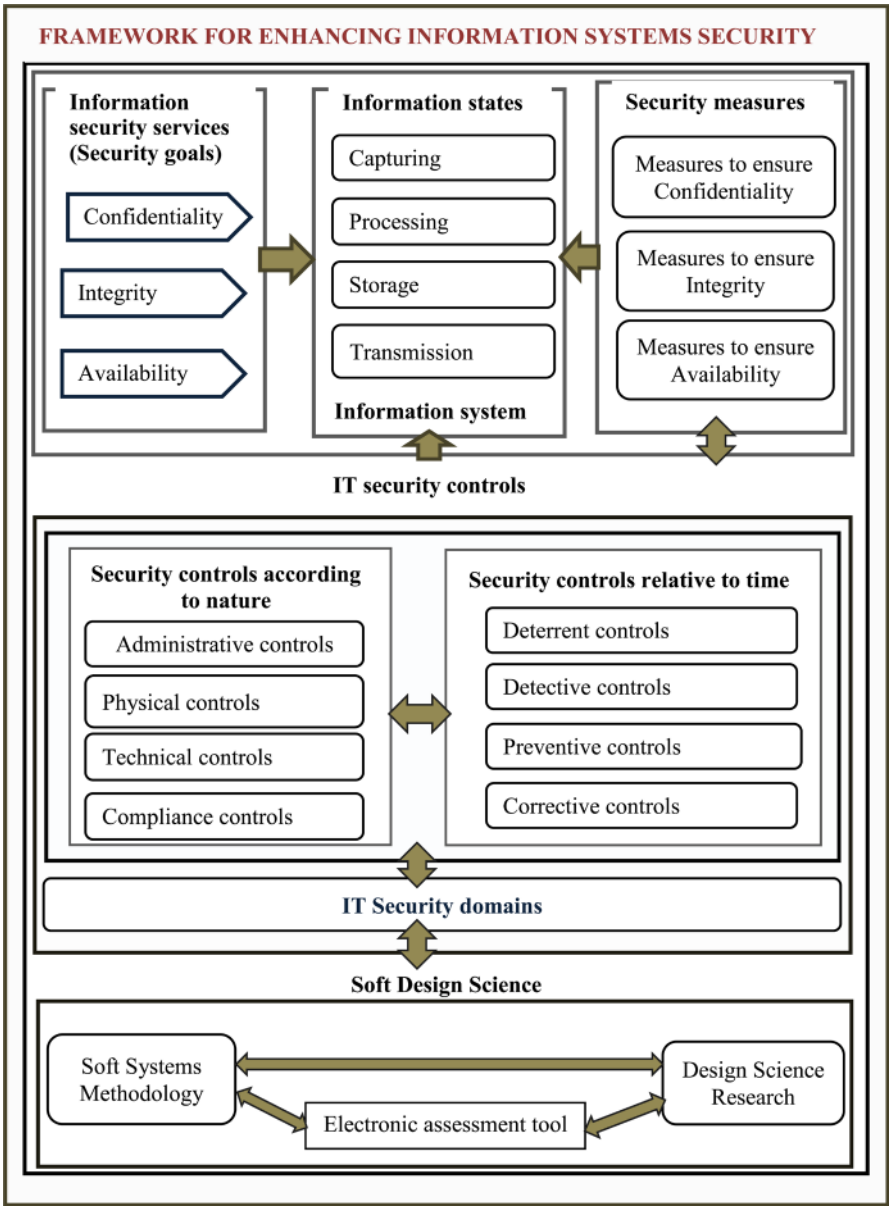


Figure 6. Proposed framework for enhancing information systems security.

thorized disclosure of contents. Maintaining confidentiality requires that data cannot be viewed by unauthorized persons and thus cannot be compromised. Data confidentiality implies keeping data private.

b) Integrity

Integrity is the guarantee that the message sent is the one received and that the message is not intentionally or unintentionally altered. Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. The data integrity ensures that data has not been modified in transit. Integrity for data means that changes made to data are done only by authorized individuals/systems. Corruption of data is a failure to maintain data integrity.

c) Availability

Availability refers to the elements that create reliability and stability in net-

works and systems. The availability is the timely, reliable access to data and information services for authorized users. Availability is about information being accessible as needed and where needed. Availability ensures that connectivity is accessible when needed, allowing authorized users to access the network or systems.

d) Information states

Within information system, for any given moment, information is found in one or more of the four states; during capturing, processing, storage, and transmission. The security requirements for ensuring the security of information in information systems; should be defined in each information states. This is consistent with [16] who created a model framework, NSTISSC Security Model (The McCumber Cube) for establishing and evaluating information.

e) Security measures

Security measures are the course of action taken to achieve a particular purpose, a procedure, initiative, operation to ensure security goals are guaranteed in information systems. Some of the identified security measures for ensuring confidentiality, integrity, and availability (CIA) of information during capturing; processing, storage, and transmission are summarized in **Table 3**.

f) IT security controls

IT Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Controls help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset. The IT security controls can be grouped according to nature or relative to time. These controls when grouped according to nature: administrative controls, physical controls, technical controls, and compliance controls. These controls when grouped relative to time: deterrent controls, detective controls, preventive controls and corrective control. Some of these IT security controls for ensuring security goals (CIA) are summarized in **Table 4**.

g) Soft Design Science Methodology

The Soft Design Science Methodology merges the common Design Science Research (DSR) process together with the iterative Soft Systems Methodology (SSM). In the proposed framework for enhancing information systems security, Soft Design Science Methodology was integrated with electronic assessment tool[1] adapted from [54]. This assessment tool evaluates the maturity level of information systems security based on security controls and security measures in each security domain. The Soft Design Science Methodologydetermines the feasible and desirable change for improvement.

7. Research Study Contributions

The main objective of this study was to tackle the wicked, complex problematic situation on how information systems security can be improved. The contributions towards this research goal are in line with the results presented in this pa-

[1]https://net.educause.edu/ir/library/excel/HEISCtool.xlsm

Table 3. Security measures for ensuring security goals (CIA).

S/N	Security measures	Descriptions	Information states				Security goals(CIA)		
			Capturing	Processing	Storage	Transmission	Confidentiality	Integrity	Availability
i	Access control mechanisms	Implement selective restriction of access to a place or information resources such as audit logs and systems logs.	√	√	√	√	√	√	
ii	Configuration management	Ensure correct configuration implementation for the information systems and ICT devices.	√	√	√	√	√	√	√
iii	Disabling/blocking insecure services, protocols/ports.	Disable or block insecure services, protocols, ports.	√	√	√	√	√		
iv	Encryption of information/data	Encrypt sensitive information/data.	√	√	√	√	√		
v	Identification and authentication	Use a unique user account and password (something you know); security token such as smartcard (something you have); biometric (something your).	√	√	√	√	√		
vi	Logging, monitoring of logs and alerting	Implement automatically logging, monitoring and alerting of security related activities regularly.	√	√	√	√	√	√	
vii	Media sanitization	Clearing, purging & destruction of data remanence prior disposal.	√	√	√	√	√		
viii	Network segmentation	Split network into subnets, VLANs; physical separation of LANs	√	√	√	√	√		
ix	Patch management	Regularly patch the applications, operating systems, and ICT devices	√	√	√	√	√	√	√
x	Security awareness and training	Conduct security awareness and training for non-disclosure of sensitive information.	√	√	√	√	√		
xi	Audit trail	Implement and monitor audit trail (audit log) for a given sensitive information system.	√	√	√	√		√	
xii	Change management for ISs	Implement change management and those changes should be documented, communicated, authorized, tested, implemented, monitored and audited to ensure the integrity of information.	√	√	√	√		√	√
xiii	Checksum (or hash sum)	Implement checksum such as MD5/SHA3 to verify the integrity of data.	√	√	√	√		√	
xiv	Digital signature	Implement digital signature to validate the authenticity and integrity of a message, software or digital document.	√	√	√	√		√	
xv	Integrity monitoring tools	Implement integrity monitoring tools for alerting of any unauthorized modification.	√	√	√	√		√	
xvi	Least privilege principle/Need to know principle	Implement procedures for reviewing users' access regularly, and only needed privileges should be applied and documented.	√	√	√	√		√	
xvii	Rotation of duties principle	Practice job rotation to breaks up opportunities for collusion and fraudulent activities.	√	√	√	√		√	
xviii	Segregation of duties principle	Duties should be sufficiently segregated in a given organization to ensure the detection of unintentional or unauthorized modification of information.	√	√	√	√		√	
xix	Backup strategies	Implement backup strategies' based on required point objective (RPO): loss acceptable; and required time objective (RTO): time required to restore ISs to operation after disaster or emergency.	√	√	√	√			√

Continued

xx	Business continuity plan(BCP)	Implement BCP; document and test regularly the BCP; no insurance that operations ever be restored to their present state in case of disaster.	√	√	√	√		√
xxi	Capacity planning	Predict and estimate the demand for information resources.	√	√	√	√		√
xxii	Data backup process	The frequency of backup; labelling; retention period; the frequency of backup rotation.	√	√	√	√		√
xxiii	Disaster recovery plan	Document; specify procedures to be followed in case of anevent of a disaster.	√	√	√	√		√
xxiv	Fault tolerance	Implement hardware and software redundancy; software recovery.	√	√	√	√		√
xxv	Incident management and response	Implement incident handling procedures; Functional incident response team and proper reporting.	√	√	√	√		√
xxvi	Monitoring of wired(LAN/WAN) and wireless networks	Continuously monitor of LAN/WAN and wireless networks for unauthorized access.	√	√	√	√	√	√
xxvii	Preventive maintenance	Regularly patching, updating antiviruses' anti-malwares, Operating systems.	√	√	√	√		√
xxviii	Protecting critical hardware and wiring from threats	Implement preventative measures to protect critical hardware and wiring from natural and man-made threats.	√	√	√	√		√
xxix	System monitoring mechanisms	Implement systems monitoring mechanisms.	√	√	√	√		√
xxx	Testing of the restore procedures	Test the restore procedures regularly.	√	√	√	√		√

Source: adapted from [14] [19] [20].

Table 4. Summary of IT security controls.

				Controls category				
					Controls relative to time			
S/N	**IT security domain**	**Security controls measures**	**Information States**	**According to nature**	**Deterrent**	**Detective**	**Preventive**	**Corrective**
i.	Information security policy	Information Security Policy approved by the top executive or board of trustee; and operational.	Capturing, Processing, Storage, Transmission	Administrative control	√	√	√	√
ii.	Organisational of information security	Chief Information Security Officer (CISO) or equivalent job responsibilities assigned.	Capturing, Processing, Storage, Transmission	Administrative control	√	√	√	√
ii (a)	Internal organisation	Roles and responsibilities allocated to individuals	Capturing, Processing, Storage, Transmission	Administrative control	√	√	√	√
ii (b)	Mobile devices and teleworking	Policies and controls for mobile devices (such as laptops, tablet PCs, wearable)	Capturing, Processing, Storage, Transmission	Administrative control	√	√	√	√
iii.	Human resources security	Policy for human resources security in place.	Capturing, Processing, Storage, Transmission	Administrative control	√	√	√	√
iv.	Asset management	Asset management Policy in place.	Capturing, Processing, Storage, Transmission	Administrative control	√	√	√	√
iv (a)	Information classification and labelling	Information classified and labelled according to the security protection needed, and handled appropriately.	Capturing, Processing, Storage, Transmission	Administrative control	√	√	√	√

Continued

iv (b)	Media handling	-Secure deletion -Destroying or degaussing physical media -Secure disposal or re-use of media	Capturing, Processing, Storage, Transmission	Technical control	√	√	√	√
v.	Access control	Access control policy in place.	Capturing, Processing, Storage, Transmission	Administrative control	√	√	√	√
v (a)	Business requirements of access	-Clearly documented -Restrict network access and connections	Capturing, Processing, Storage, Transmission	Technical control	√	√	√	√
vi.	Cryptography	Cryptographic policy in place.	Capturing, Processing, Storage, Transmission	Administrative control	√	√	√	√
vi (a)	Encryption	Encryption ofdata/information	Capturing, Processing, Storage, Transmission	Technical control	√	√	√	√
vi (b)	Cryptographic authentication and integrity	-Digital signature; -Message authentication code; -Checksum (cryptographic hash function); -Non-repudiation; -Cryptographic key management.	Capturing, Processing, Storage, Transmission	Technical control	√	√	√	√
vii.	Physical and environmental security	Physical security policy in place.	Capturing, Processing, Storage, Transmission	Administrative control	√	√	√	√
vii (a)	Physical security perimeter	-Securing offices, rooms and facilities. -Public access, delivery and loading areas; doors, lock, electric fence, CCTV, smartcard, biometric (e.g. fingerprint).	Capturing, Processing, Storage, Transmission	Physical control	√	√	√	√
vii (b)	Protecting against external and environmental threats	-Protecting against fires, floods, earthquakes, bombs, etc. -Climate protecting system, fire suppression system	Capturing, Processing, Storage, Transmission	Physical control	√	√	√	√
vii (c)	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	Capturing, Processing, Storage, Transmission	Physical control	√	√	√	√
viii.	Operations Security	Operations security policy in place	Capturing, Processing, Storage, Transmission	Administrative control	√	√	√	√
viii (a)	Multi-factor authentication	Something you know (PIN/Password)/ something you have (ATM/Smartcard)/ something you are (Biometric, e.g. fingerprint).	Capturing, Processing, Storage, Transmission	Technical control	√	√	√	√
ix.	Communications and operations management	Communications and operations policy in place.	Capturing, Processing, Storage, Transmission	Administrative control	√	√	√	√
ix (a)	Network security management	-Networks and network services should be secured; -Network segmentation/segregation.	Capturing, Processing, Storage, Transmission	Technical control	√	√	√	√
ix (b)	Information transfer	Policies, procedures and agreements in place (e.g. non-disclosure agreements) for information transfer to/from third parties, including electronic messaging.	Capturing, Processing, Storage, Transmission	Administrative control	√	√	√	√
x.	System acquisition, development and maintenance	System acquisition, development and maintenance policy in place.	Capturing, Processing, Storage, Transmission	Administrative control	√	√	√	√
x (a)	Security requirements of information systems	Security control requirements should be analysed and specified.	Capturing, Processing, Storage, Transmission	Administrative control	√	√	√	√

Continued

xi.	Supplier relationships	Supplier relationships policy in place.	Capturing, Processing, Storage, Transmission	Administrative control	√	√	√	√
xii.	Information security incident management	Information security incident management policy in place.	Capturing, Processing, Storage, Transmission	Administrative control	√	√	√	√
xii (a)	Management of information security incidents and improvements	There should be responsibilities and procedures to manage (report, assess, respond to and learn from) information security events, incidents and weaknesses consistently and effectively, and to collect forensic evidence.	Capturing, Processing, Storage, Transmission	Administrative control	√	√	√	√
xiii.	Information security aspects of business continuity management	Business continuity plan document in place.	Capturing, Processing, Storage, Transmission	Administrative control	√	√	√	√
xiii (a)	Redundancies	IT facilities should have sufficient redundancy to satisfy availability requirements.	Capturing, Processing, Storage, Transmission	Technical control	√	√	√	√
xiv.	Compliance	Compliance policy in place.	Capturing, Processing, Storage, Transmission	Administrative control	√	√	√	√
xiv (a)	Compliance with legal and contractual requirements	The organisation must identify and document its obligations to external authorities and other third parties in relation to information security.	Capturing, Processing, Storage, Transmission	Compliance control	√	√	√	√
xv.	Risk Management	Risks registered developed, operational and updated.	Capturing, Processing, Storage, Transmission	Compliance control	√	√	√	√

Source: adapted from [13] [14] [19] [20].

per. This research has several practical contributions. Firstly, it contributes to the body of knowledge of information systems security by providing a set of security requirements for ensuring information systems security. Secondly, it contributes empirical evidence on how information systems security can be improved. Thirdly, it contributes on the applicability of Soft Design Science Methodology in addressing the problematic situation in information systems security. Fourthly, this research provides a framework for enhancing information systems security during capturing, processing, storage and transmisstion of information.

8. Conclusions and Recommendations

In addressing the research problem, the study assessed security requirements and proposed a framework for improving the security of information systems using multi-layered security approach integration with Soft Design Science Methodology. In addition, Soft Design Science Methodology was compounded with mixed research methodology (*i.e.* qualitative and quantitative research methodology were used). This holistic approach helped for research methodology triangulation. In order to test the validity of the proposed framework for enhancing ISS, the systems requirements were collected using both structured systems analysis and design, and object oriented analysis and design principles.

The study carried out maturity level assessment for security status quo to determine security requirements gap (IT security controls, IT security measures). For assessing the security status quo, the study applied SSE-CMM with a rating scale of 0 - 5 to determine the maturity level. The study found that maturity level across security domain is 0.44 out of 5 in SSE-CMM rating scale 0 - 5 in the education sector in Tanzania. The finding shows that implementation of security controls and security measures for ensuring security goals for each security requirement domain are lacking or practiced in ad-hoc. Thus, for improving the security of information during capturing, processing, storage, and transmission in information systems, organisations should implement security controls and security measures for ensuring security goals for each security domain (multi-layer security: security defence in depth approach).The research recommends further research work in an empirical study to test the applicability of the proposed framework for enhancing information systems security during processing, storage, and transmission of information; in other sectors such as banking industry, and healthy sector. Also, further research work is recommended in hardening information security in the education sector in Tanzania using Human Sensor Web for Crowd sourcing security incidents.

References

[1] Nfuka, E.N., Sanga, C. and Mshangi, M. (2014) The Rapid Growth of Cybercrimes Affecting Information Systems in the Global : Is this a Myth or Reality in Tanzania ? *International Journal of Information Security Science*, **3**, 182-199. http://www.ijiss.org/ijiss/index.php/ijiss/article/view/72

[2] Mshangi, M., Nfuka, E.N. and Sanga, C. (2015) Using Soft Systems Methodology and Activity Theory to Exploit Security of Web Applications against Heartbleed Vulnerability. *International Journal of Computing and ICT Research*, **8**, 32-52. http://ijcir.mak.ac.ug/volume8-number2/article4.pdf

[3] Mshangi, M., Nfuka, E.N. and Sanga, C. (2016) Designing Secure Web and Mobile-Based Information System for Dissemination of Students' Examination Results : The Suitability of Soft Design Science Methodology. *International Journal of Computing and ICT Research*, **10**, 10-40. http://ijcir.mak.ac.ug/volume10-issue2/article2.pdf

[4] Sherwood, J., Clark, A. and Lynas, D. (2009) Enterprise Security Architecture. *SABSA White Paper*, **6**, 43-54.

[5] Wihitmen, M. and Mattord, H. (2012) Principles of Information Security. 4th Edition, Cengage Learning, Boston. http://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf

[6] Krutz, R.L. and Vines, R. (2007) The CISSP and CAP Prep Guide (Platinum E). Wiley Publishing Inc., New Delhi.

[7] Lacey, D. (2009) Managing the Human Factor in Information Security : How to Win Over Staff and Influence Business Managers. John Wiley & Sons Ltd., Chichester. https://www.amazon.com/Managing-Human-Factor-Information-Security/dp/0470721995

[8] Nachtigal, S. (2009) E-Business Information Systems Security Design Paradigm and Model. The University of London, London.

http://digirep.rhul.ac.uk/items/bf2711d5-4654-40ee-b1c6-4b4f0f83ac97/1/

[9] Rupere, T., Mary, M. and Zanamwe, N. (2012) Towards Minimizing Human Factors in End-User Information Security. *International Journal of Computer Science and Network Security*, **12**, 159-167.

[10] Soltanmohammadi, S., Asadi, S., Ithnin, N. and Science, C. (2013) Main Human Factors Affecting Information System Security Seed. *Interdisciplinary Journal of Contemporary Research in Business*, **5**, 329-354. http://ijcrb.webs.com/

[11] Symantec (2016) Internet Security Threat Report. Network Security.

[12] Bakari, J.K. (2007) A Holistic Approach for Managing ICT Security in Non-Commercial Organisations: A Case Study in a Developing Country. PhD Thesis. Stockholm University.
http://www.diva-portal.org/smash/get/diva2:197030/FULLTEXT01.pdf

[13] ISO/IEC 27001:2013 (2013) ISO/IEC 27001:2013 Information Technology Security Techniques Information Security Management Systems Requirements.
http://www.iso.org/iso/catalogue_detail?csnumber=54534

[14] ISO/IEC 27002:2013 (2013) ISO/IEC 27002:2013 Information Technology Security Techniques Code of Practice for Information Security Controls.
http://www.iso.org/iso/catalogue_detail?csnumber=54533

[15] Mbowe, J.E., Msanjila, S.S., Oreku, G.S. and Kalegele, K. (2016) On Development of Platform for Organization Security Threat Analytics and Management (POSTAM) Using Rule-Based Approach. *Journal of Software Engineering and Applications*, **9**, 601-623. https://doi.org/10.4236/jsea.2016.912041

[16] McCumber, C.J.R. (1991) Information Systems Security: A Comprehensive Model. *The* 14*th National Computer Security Conference*, Washington DC, 1-4 October 1991, 328-337.
http://csrc.nist.gov/publications/history/nissc/1991-14th-NCSC-proceedings-vol-1.pdf

[17] Microsoft (2002) The STRIDE Threat Model.
https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20)aspx

[18] Microsoft (2015) Microsoft Advanced Threat Analytics.
https://www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics

[19] PCI-DSS (2013) Payment Application Data Security Standard Requirements and Security Assessment Procedures.
https://www.pcisecuritystandards.org/minisite/en/docs/PA-DSS_v3.pdf

[20] PCI-DSS (2016) Data Security Standard. Security.
https://pcicompliance.stanford.edu/sites/default/files/pci_dss_v3-2.pdf

[21] Roessing, R.M. (2010) The Business Model for Information Security. *ISACA Journal*, 1-27.
https://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf

[22] SAN (2013) Interested in learning SANS Institute InfoSec Reading Room Layered Security : Why It Works Layered Security : Why It Works. SAN Institute, 1-13.
https://www.sans.org/reading-room/whitepapers/analyst/layered-security-works-34805

[23] Al-Azazi, S. (2008) A Multi-Layer Model for E-Government Information Security Assessment. http://hdl.handle.net/1826/3182

[24] Shaaban, H.K. (2014) Enhancing the Governance of Information Security in Developing Countries: The Case of Zanzibar. PhD Thesis, Bedfordshire.
http://uobrep.openrepository.com/uobrep/bitstream/10547/315359/1/Hussein-Shaaban-PhD-Thesis.pdf

[25] Arcidiacono, G. (2014) Feature Challenges and Benefits of Migrating to COBIT 5 in the Strongly Regulated Environment of EU Agricultural Paying Agencies. *ISACA Journal*, **1**, 1-3. https://www.isaca.org/Journal/archives/2014/Volume-1/Documents/Challenges-and-Benefits-of-Migrating-to-COBIT-5_joa_Eng_0114.pdf

[26] ISACA (2012) COBIT 5 for Information Security. *ISACA Journal*, **1**. http://www.isaca.org/cobit/pages/info-sec.aspx

[27] Techopedia (2017) Layered Security. https://www.techopedia.com/definition/4005/layered-security

[28] Baskerville, R., Pries-Heje, J. and Venable, J. (2009) Soft Design Science Methodology. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*, 1-11.

[29] Peffers, K.E.N., Rothenberger, M. and Kuechler, B. (2012) Design Science Research in Information Systems Advances in Theory and Practice. *7th International Conference*, Las Vegas, May 2012. https://doi.org/10.1007/978-3-642-29863-9

[30] Peffers, K.E.N., Tuunanen, T., Rothenberger, M. and Chatterjee, S. (2007) A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, **24**, 45-77. https://doi.org/10.2753/MIS0742-1222240302

[31] Sanga, C. (2010) A Technique for the Evaluation of Free and Open Sources E-Learning Systems. PhD Thesis, The University of the Western Cape. http://etd.uwc.ac.za/xmlui/bitstream/handle/11394/2564/Sanga_PHD_2010.pdf?sequence=1

[32] Farrell, R. and Hooker, C. (2013) Design, Science, and Wicked Problems. *Design Studies*, **34**, 681-705.

[33] Gregor, S. and Hevner, A.R. (2013) Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly*, **37**, 337-355. http://www.misq.org/skin/frontend/default/misq/pdf/appendices/2013/V37I2_Appendices/GregorHevnerAppendices.pdf

[34] Hevner, A.R. and Chatterjee, S. (2012) Design Research in Information Systems: Theory and Practice. Vol. 28, Springer, Berlin.

[35] Mahundu, F.G. (2016) E-Governance: A Sociological Case Study of the Central Admission System in Tanzania. *The Electronic Journal of Information Systems in Developing Countries*, **79**, 1-11. http://www.ejisdc.org/ojs2./index.php/ejisdc/article/viewFile/1742/655

[36] Hevner, A.R., March, S., Park, J. and Ram, S. (2004) Design Science Research in Information Systems. *Management Information Systems Quarterly*, **28**, 75-105.

[37] Mahundu, F.G. (2015) E-Governance in the Public Sector: A Case Study of the Central Admission System in Tanzania. PhD Thesis. Rhodes University. http://contentpro.seals.ac.za/iii/cpro/DigitalItemViewPage.external?lang=eng&sp=1020845&sp=T&suite=def

[38] Basden, A. (2003) Reflections on CATWOE, a Soft Systems Methodology Technique for Systems Designs. *Information Systems Journal*, **17**, 55-73.

[39] Checkland, P.B. and Scholes, J. (1990) Soft Systems Methodology in Action. John Wiley & Sons, Inc., New York. http://dl.acm.org/citation.cfm?id=130360

[40] Novani, S., Putro, U.S. and Hermawan, P. (2014) An Application of Soft System Methodology in Batik Industrial Cluster Solo by Using Service System Science Perspective. *Procedia—Social and Behavioral Sciences*, **115**, 324-331.

[41] Checkland, P.B. (1998) Systems Thinking, Systems Practice. John Wiley & Sons

Ltd., Hoboken.

[42] Salner, M. and Ph, D. (1999) Beyond Checkland & Scholes : Improving SSM. *I Can*, **11**, 20. http://www.systemdynamics.org/conferences/1999/PAPERS/PLEN3.PDF

[43] Graham, W. (1989) Action and Research : A Soft Systems approach to Organisational Development Evaluating Soft Systems & Organisational Development.

[44] Williams, B. and Hof, S. (2014) Wicked Solutions: A Systems Approach to Complex Problems. Bob! Williams. http://www.bobwilliams.co.nz/wicked.pdf

[45] Maconachy, S. and Ragsdale, W. (2001) A Model for Information Assurance: An Integrated Approach. *Proceedings of the* 2001 *IEEE Workshop on Information Assurance and Security*, West Point, 308-310.

[46] Kimble, C. (2008) Holistic Methodologies. http://www.chris-kimble.com/Courses/sdm/Presentations/SDM7.pdf

[47] Ashford, W. (2014) The Human Factor a Key Challenge to Information Security. http://www.computerweekly.com/news/2240236390/The-human-factor-a-key-challenge-to-information-security-say-experts

[48] Futcher, L. (2011) An Integrated Risk-Based Approach to Support IT Undergraduate Students in Secure Software Development. http://dspace.nmmu.ac.za:8080/jspui/handle/10948/1673

[49] Ismail, Z., Masrom, M., Sidek, Z. and Hamzah, D. (2010) Framework to Manage Information Security for Malaysian Academic Environment. *Journal of Information Assurance & Cybersecurity*, **2010**, Article ID: 305412. https://doi.org/10.5171/2010.305412

[50] Kapis, K. (2011) Security and Privacy of Electronic Patient Records. PhD Thesis, the Open University of Tanzania.

[51] Kasita, C. and Laizer, L.S. (2013) Security Architecture for Tanzania Higher Learning Institutions' Data Warehouse. *Journal of Information & Knowledge Management*, **3**, 25-32.

[52] Davey, J.W., Gugiu, P.C. and Coryn, C.L.S. (2010) Quantitative Methods for Estimating the Reliability of Qualitative Data. *Journal of Multi Disciplinary Evaluation*, **6**, 140-162.

[53] Jick, T.D. (1979) Mixing Qualitative and Quantitative Methods : Triangulation in Action Mixing Qualitative and Quantitative Methods : Triangulation in Action. *Administrative Science Quarterly*, **24**, 602-611. https://doi.org/10.2307/2392366

[54] EDUCASE (2015) Assessment Tool—Educause. https://library.educause.edu/~/media/files/library/2015/11/heisctool-xlsm.xlsm

[55] Cohen, L., Manion, L. and Morrison, K. (2007) Research Methods in Education. Professional Development in Education, 6th Edition, Vol. 38, Routledge, New York.

[56] Saunders, M.N.K., Lewis, P., Thornbill, A. and Jenkins, M. (2009) Research Methods for Business Students. 5th Edition, Pearson Education Limited.

[57] PMO-RALG (2016) The Prime Minister's Office, Regional Administration and Local Government (PMO-RALG). http://www.tamisemi.go.tz/

[58] WEST (2016) Ministry of Education, Science, and Technology (WEST): Institutions. http://moe.go.tz/index.php/sw/

[59] ISO/IEC 21827:2008 (2008) ISO/IEC 21827:2008 Information Technology Security Techniques—Systems Security Engineering Capability Maturity Model (SSE-CMM). http://www.iso.org/iso/catalogue_detail.htm?csnumber=44716

[60] Lacey (2013) Factor Analysis Using R. *Practical Assessment, Research, and Evaluation*, **18**, 1-11. http://pareonline.net/pdf/v18n4.pdf

[61] R Development Core Team (2005) What Is R? https://www.r-project.org/about.html

[62] Tavakol, M. and Dennick, R. (2011) Making Sense of Cronbach's Alpha. *International Journal of Medical Education*, **2**, 53-55. https://doi.org/10.5116/ijme.4dfb.8dfd

[63] Cronbach, L.J. (1951) Coefficient Alpha and the Internal Structure of Tests. *Psychometrika*, **16**, 297-334. https://doi.org/10.1007/bf02310555

[64] Smyth, D.S. and Checkland, P.B. (1976) Using a Systems Approach: The Structure of Root Definitions. *Journal of Applied Systems Analysis*, **5**, 75-83.

[65] Maqood, T., Finegan, A.D. and Walker, D.H. (2001) Five Case Studies Applying Soft Systems Methodology to Knowledge Management. QUT Digital Repository. http://eprints.qut.edu.au/27456/

[66] Cundill, G., Cumming, G.S., Biggs, D. and Fabricius, C. (2012) Soft Systems Thinking and Social Learning for Adaptive Management. *US National Library of Medicine National Institutes of Health*, **1**, 13-20. http://www.ncbi.nlm.nih.gov/pubmed/22060320

[67] Timurtas, D. (2011) Can an Integration of Soft Systems Methodology & the Ethics Framework Enhance Socio-Technical Systems Design in Large and Complex Organizations ? An Action Research Study on Two NHS Pathways and Their Design Strategies. https://www.ucl.ac.uk/silva/uclic/studying/taught-courses/distinction-projects/2010_theses/TimurtasD.pdf

[68] Razali, S., Noor, N.L.M. and Adnan, W.A.W. (2010) Applying Soft System Methodology (SSM) into the Design Science: Conceptual Modeling of Community Based E-Museum (ComE) Framework. *IEEE International Conference on Systems, Man and Cybernetics*, 2701-2707.